

The Patent Bulletin, Republic of China [19] [12]

[11] The bulletin no: 428163

[44] Invented in Republic of China, April 1, 2001    Total 4 pages

[51] Int Cl    G11B2D/00  
                 G11B7/007  
                 G11B7/013

---

[54] The patent name: A recorded information copy protection system

[21] The application no: 087102808                      [22] The application date: February 26, 1998

[72] The inventor: A person associated with a Dutch company

[71] The applicant: Royal Philips Electronics Co. Ltd, Holland

[74] The agent: Mr. Chen Changwen

[57] The scope of the patent to be applied for:

1. A recorded information copy protection system is fitted with an information carrier with a central mark. The central mark represents the first position of the meta-model (x). A recording device can record information on the information carrier; while a playing device can play back recorded information on the information carrier. The recorded information features a watermark representing the second position of the meta-model (y). The second position of the meta-model is related to the first position. It includes a coding mechanism (23), which imbeds the watermark into the information, as well as a generating mechanism. The generating mechanism can generate the second position meta-model based on the correlation between the first position and second position meta-models. The playback device encompasses a confirmation mechanism (29), which can identify and confirm the correlation between the first position and the second position meta-models.

2. If the patent application scope is for the system in the first item, it encompasses the correlation including a one way coding function.

3. If the patent application scope is for the system in the second item, it is related to integrating the one-way function into the first position meta-model (x) to generate the second meta-model (y).

4. If the patent application scope is for the systems in the first, second and third items, it is related to the confirming and coding mechanisms of the second position meta-model.

5. The recording device used in the first, second and third items in the patent application scope is able to record information on the information carrier, which embodies one central mark representing the first position meta-model (x). The recording device encompasses a coding mechanism (23), which imbeds the watermark into the information. The watermark represents the second position meta-model (y), while the generator is able to generate the

second position meta-model based on the correlation between the first and second meta-models.

6. If the patent application scope is for the recording device in the fifth item, it encompasses a marking mechanism (46), which is able to create a central mark in the information carrier, while the generator encompasses the first position meta-model mechanism which produces crystals based on the pre-determined information correlation (44).

7. If the patent application scope is for the recording device in the sixth item, it is concerned with the integration utilization of the generator in that the first part represented by the pre-compressed mark on the information carrier of the recordable data is combined with the second part (x) generated by crystals to produce the first position meta-model (x).

8. If the patent application scope is for the recording device in the seventh item, it is concerned with the pre-determined correlation which encompasses a one way function.

9. If the patent application scope is for the information carrier used in the systems of the first, second and third items, then the information carrier (51) encompasses one recorded information as well as the central mark (50) representing the first meta-model. The recorded information embodies the watermark representing the second meta-model. This watermark pre-determines the correlation for the first position meta-model.

10. If the patent application scope is for the information carrier in the ninth item, its characteristics lie in the fact that the first position meta-model encompasses the first part (x) of the source of the identifiable information carrier as well as the identifiable second part.

11. The playback device, used in the patent application scope for the system in the first, second or third items, is able to re-create the information in the information carrier (51). It also embodies the mechanism (50), which can identify the central mark. This central mark represents the first position meta-model (x). This playback device embodies a watermark reading mechanism (55), which can identify the second position meta-model in the recorded information represented by the watermark.

12. If the patent application scope is for the playback device in the eleventh item, it is concerned with the confirmation device, including a one way code diagram (53).

13. If the patent application scope is for the information carrier in the twelfth item, it is concerned with the programming confirmation device, which generates the confirmation model (y). In this application, the one way function is utilized in the first position meta-model (x), together with the comparable devices (54) in the confirmation model (y) and the second position meta-model (y).

The simple explanation for the diagram:

The first diagram shows the conditional replay rules.

The second diagram shows the recording protection for the recording device, the central mark as well as the playback device.

The third diagram shows the one way function.

The fourth diagram shows the recording device.

The fifth diagram shows the playback device.

[11]公告編號：428163

[44]中華民國 90 年 (2001) 04 月 01 日  
發明

全 4 頁

[51] Int.Cl 06: G11B20/00  
G11B7/007  
G11B7/013

[54]名稱：供已錄製信號拷貝保護之系統

[21]申請案號：087102806

[22]申請日期：中華民國 87 年 (1998) 02 月 26 日

[72]發明人：

強森保羅馬利傑瑞德林納茲 荷蘭

[71]申請人：

皇家飛利浦電子股份有限公司 荷蘭

[74]代理人：陳長文 先生

1

[57]申請專利範圍：

1. 一種已錄製資訊之拷貝保護的系統，包括一含中央標記的資訊載體，該中央標記代表第一位元模型(x)，一錄製器可在資訊載體上錄製資訊，而播放器可重製資訊載體上的已錄製的資訊，其特徵在於已錄製的資訊包括代表第二位元模型(y)的一水印，該第二位元模型與第一位元模型相關，該第二位元模型包括一編碼器裝置(23)，可將水印嵌入資訊中，及一產生器裝置(25)，可依第一與第二位元模型的關連性產生第二位元模型，該播放器包括一確認裝置(29)，可確認第二位元模型與第一位元模型之間的關連性。
2. 如申請專利範圍第1項的系統，其特徵在於其關連性包括一密碼單向功能。
3. 如申請專利範圍第2項的系統，其特徵在於利用提供單向功能至第一位元模型(x)而產生第二位元模型(y)。
4. 如申請專利範圍第1，2，或3項的系

2

- 統，其特徵在於第二位元模型確認編碼器裝置。
5. 一種使用在申請專利範圍第1，2或3項系統中的錄製器，可在資訊載體上錄製資訊，該資訊載體包括一中央標記，代表第一位元模型(x)，其特徵在於錄製器包括編碼器裝置(42)，可將水印嵌入資訊中，該水印代表第二位元模型(y)，而產生器裝置(43)可依第一與第二位元模型之間的關連性而產生第二位元模型。
10. 6. 如申請專利範圍第5項的錄製器，其特徵在於包括一標記裝置(46)，可在資訊載體上建立中央標記，而產生器包括可依預定的關連性來產生子晶(u)的第一位元模型的裝置(44)。
15. 7. 如申請專利範圍第6項的錄製器，其特徵在於產生器(43)利用結合，由在可錄製的資訊載體的預壓縮的標記表示之第一部份(x)與由子晶(u)所產生的第二
- 20.

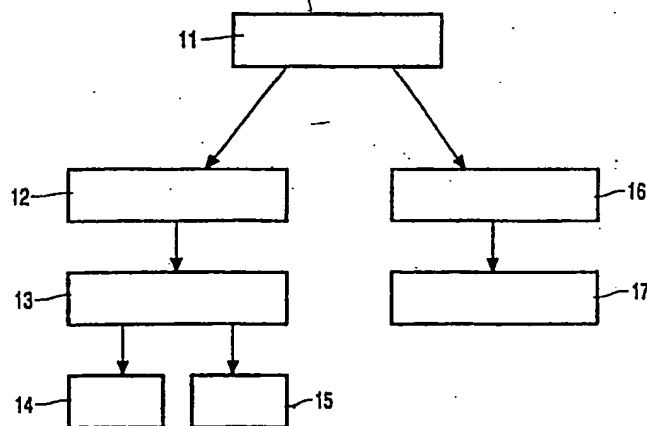
(2)

3

- 部份( $x_1$ )來產生第一位元模型( $x$ )。
- 8.如申請專利範圍第7項的錄製器，其特徵在於預定關連性包括一密碼單向功能。
- 9.一種用於申請專利範圍第1、2或3項系統的資訊載體，該資訊載體(51)包括一已錄製的資訊與一代表第一位元模型( $x$ )的中央標記(50)，其特徵在於已錄製的資訊包括一代表第二位元模型( $y$ )的水印，該水印對第一位元具預先定義的關連性。
- 10.如申請專利範圍第9項的資訊載體，其特徵在於第一位元模型包括可確定資訊載體的來源的第一部份( $x_1$ )，與可確認( $x_t$ )的第二部份。
- 11.一種用於申請專利範圍第1、2或3項系統的播放器，可重製資訊載體(51)的資訊，並包括可偵測出中央標記的裝置(50)，該中央標記代表第一位元模型( $x$ )，其特徵在於該播放器包括一水印讀取裝置(55)，可偵測由在錄製資訊中

4

- 的水印所代表的第二位元模型( $y$ )，而在此情形下，該播放器包括確認裝置(53、54)可確認第二位元模型與第一位元模型之間的預定關係。
5. 12.如申請專利範圍第11項的播放器，其特徵在於認證裝置包括一密碼圖表單向功能(53)。
- 13.如申請專利範圍第12項的播放器，其特徵在於編程認證裝置，來產生確認模型( $y'$ )，只要利用將單向功能運用到第一位元模型( $x$ )，並包括可比較確認模型( $y'$ )與第二位元模型( $y$ )的裝置(54)。
- 圖式簡單說明：
15. 第一圖說明條件性的重播規則，  
第二圖說明包括錄製器、中央標記、與播放器的錄製保護，  
第三圖說明單向功能，  
第四圖說明錄製器，與  
第五圖說明播放器。

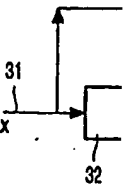


第一圖

21

22

u



第

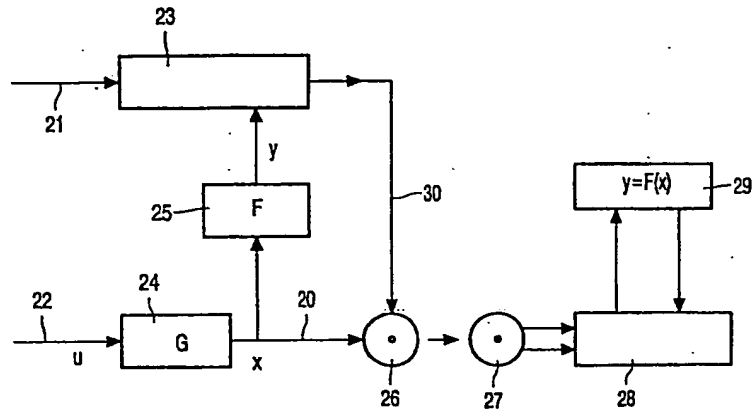
(3)

元模型(y)，而  
包括確認裝置  
元模型與第一  
係。

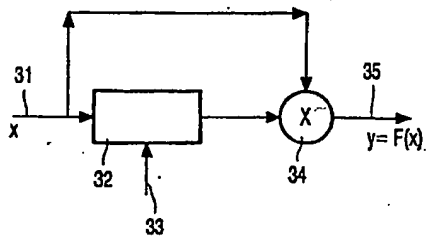
頁的播放器，其  
一密碼圖表單

頁的播放器，其  
來產生確認  
向功能運用至  
括可比較確認  
模型(y)的裝置

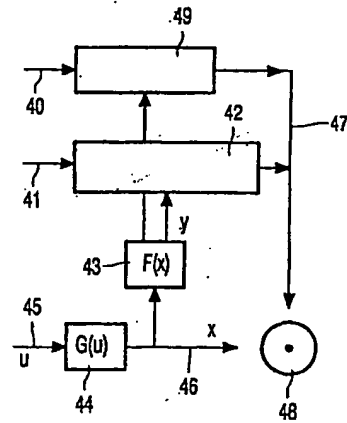
重播規則，  
製器、中央標  
，  
，  
與



第二圖

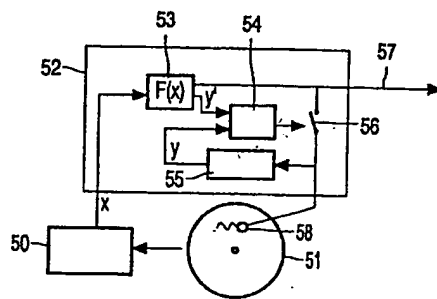


第三圖



第四圖

(4)



第五圖

[11]公告編號：428

[44]中華民國 90

[51] Int.Cl. 06: G

[54]名稱：光碟機

[21]申請案號：01

[72]發明人：

柯朝元

吳宗鴻

黃安穎

[71]申請人：

財團法人工業

[74]代理人：

[57]申請專利範圍

1.一種光碟機傳動

中，該碟機至

置、一讀寫模

一齒輪組，分

其中該齒輪組

碟片承載裝置

包括：

一轉輪，配置

一斜板，配置

由該轉輪帶動

制面，分別與

該舉升面係用

碟片讀寫位置

讀寫模組降低

一齒輪，配置

與該齒輪組耦

以帶動該轉輪，

2.如申請專利範圍

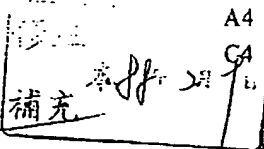
動裝置，其中

於該轉輪之部

# 公告本

申請日期	87. 2. 26.
案 號	87102806
類 別	G11B 20/00, 7/007, 7/013

(88年2月修正頁)



428163

(以上各欄由本局填註)

發 明 專 利 說 明 書		
一、發明 名稱	中 文	供已錄製信號拷貝保護之系統
	英 文	"SYSTEM FOR COPY PROTECTION OF RECORDED SIGNALS"
二、發明 創作人	姓 名	強森 保羅 馬利 傑瑞德 林納茲
	國 籍	荷蘭
	住、居所	荷蘭恩特荷芬市格諾內梧茲路1號
三、申請人	姓 名 (名稱)	荷蘭商皇家飛利浦電子股份有限公司
	國 籍	荷蘭
	住、居所 (事務所)	荷蘭愛因和文市格羅尼渥街1號
	代 表 人 姓 名	J · G · A · 羅夫斯

經濟部中央標準局員工消費合作社印製

裝

訂

線



# 公告本

申請日期	87. 2. 26.
案 號	87102806
類 別	G11B 20/00, 7/007, 7/013

(88年2月修正頁)

補充	本	冊	20	94	1
----	---	---	----	----	---

428163

(以上各欄由本局填註)

發 明 專 利 說 明 書		
一、發明 名稱	中 文	供已錄製信號拷貝保護之系統
	英 文	"SYSTEM FOR COPY PROTECTION OF RECORDED SIGNALS"
二、發明 創作人	姓 名	強森 保羅 馬利 傑瑞德 林納茲
	國 籍	荷蘭
	住、居所	荷蘭恩特荷芬市格諾內梧茲路1號
三、申請人	姓 名 (名稱)	荷蘭商皇家飛利浦電子股份有限公司
	國 籍	荷蘭
	住、居所 (事務所)	荷蘭愛因和文市格羅尼渥街1號
	代 表 人 姓 名	J · G · A · 羅夫斯

裝

訂

線

經濟部中央標準局員工消費合作社印製

428163

(由本局填寫)

承辦人代碼：
大類：
I P C分類：

A6  
B6

本案已向：

國(地區) 申請專利，申請日期： 案號： ☐有 ☐無主張優先權

歐盟

1997年1月27日

97200165.5

☐有 ☒無主張優先權

有關微生物已寄存於：

，寄存日期：

，寄存號碼：

(請先閱讀背面之注意事項再填寫本頁各欄)

裝

訂

線

經濟部中央標準局員工消費合作社印製

## 四、中文發明摘要(發明之名稱: 供已錄製信號拷貝保護之系統)

本發明揭示一種供已錄製信號拷貝保護之系統，該系統包括一資訊載體，一錄製器與一播放器。資訊載體可為光學磁片，包括一代表第一位元模型的中央標記，該中央標記不能拷貝在標準錄製裝置中。已錄製的資訊包括一代表第二位元模型的水印，該第二位元模型與第一位元模型具預定關連性水印。無法在不干擾資訊重製品質的情形下複製。介於水印與中央標記之間之關連性最好是單向功能，且要求不法拷貝也會具備相對應的中央標記。由於不論是水印或中央標記均不能複製，因此可防止不法的拷貝。錄製器包括一編碼器裝置，可將水印嵌入資訊，以及一產生器，可依該關連性產生第二位元模型。播放器包括確認該關連性的認證裝置。

## 英文發明摘要(發明之名稱: "SYSTEM FOR COPY PROTECTION OF RECORDED SIGNALS")

A system for copy protection of recorded information is disclosed, comprising an information carrier, a recorder and a player. The information carrier, e.g. an optical disc, comprises a medium mark representing a first bitpattern, which medium mark cannot be copied on standard recording devices. The recorded information comprises a watermark representing a second bitpattern, which second bitpattern has a predefined relationship to the first bitpattern. The watermark cannot be manipulated without disturbing the quality of the reproduction of the information. The relationship, preferably a one-way function, between the watermark and the medium mark requires that an illegal copy also has the corresponding medium mark. As neither the watermark nor the medium mark can be manipulated, a strong protection against illegal copying is achieved. The recorder comprises encoder means for embedding the watermark in the information and generator means for generating the second bitpattern according to said relationship. The player comprises verification means for verifying said relationship.

## 五、發明說明(1)

本發明與一種保護已錄製資訊的拷貝保護系統有關，包括一含代表第一位元模型的中央標記之資訊載體，一錄製器可錄製在資訊載體的資訊，與可由資訊載體重製所錄製的資訊之播放器。

本發明更與錄製器有關，可錄製在資訊載體上的資訊，該資訊載體包括一代表位元模型的中央標記。

本發明更與資訊載體有關，該資訊載體包括已錄製的資訊以及代表位元模型的中央標記。

本發明更與播放器有關，該播放器可自資訊載體複製資訊，並包括可偵測代表位元模型的中央標記之裝置。

拷貝保護在音頻發行上具有長久的歷史。目前安裝的設備基座，包括含音效卡的PC，只能提供不法拷貝的微小保護。在許多防拷貝的計畫中，最困難的議題是盜印者可重放原磁片，他可以將磁片的内容當成是類比家用錄製片並將之錄製起來。消費錄製者應以無限制地拷貝自己的創作品，但應禁止錄製版權所有的內容。因此，拷貝機制必須能區別消費自己的創作品以及由專業音樂發行者所發行的音樂。相關設備應只依內容來制定此項區別，若參照內容的其他來源(如磁片或麥克風)都是不適當的。對於如DCC的數位儲存媒介而言，已定義了"拷貝位元"，該位元表示版權狀態，如"不能拷貝"，"自由拷貝"或"只可以拷貝一份"。其他的拷貝位元可能表示的是，中央儲存資訊必須為以按下而作成的"專業"媒介而不是"可錄製的"磁片。

(請先閱讀背面之注意事項再填寫本頁)

訂

## 五、發明說明(2)

已錄製資訊的拷貝保護系統包括一錄製器，資訊載體與播放器，揭示在EP-0545472(相關文件表的D1)。拷貝保護是建立在所謂的中央標記上的，例如代表位元模型有形標記，表示媒介的狀態，例如，一密碼表示用按下即可製造的"專業"磁片。中央標記應不能用標準設備來拷貝或改變，因此它會以不同於錄製資訊的方法被儲存在資訊載體中，如音效或影效等方法。中央標記可由播放器來偵測，且若不出現時，或表示不同狀態時(例如不法拷貝的"可錄製的磁片")，則會鎖定重製。已知的資訊載體包括預先編程的引導軌道，一個所謂的預定溝。在由預定溝所決定的磁軌中，資訊可以用預定的方法來寫入，該方法是光學可讀取式的模型，是由第一有形參數的變數來形成，如掃描表面的高度。預定溝具第二有形參數的變數，如以橫越方向進行的偏移，亦可以顫動的形式展現。顫動為FM調幅，因此調幅代表用在回復資訊的位元模型，例如回復儲存為擾頻資訊的解擾頻資訊，該位元模型組成中央標記，因為磁軌顫動不能以標準錄製設備複製至可錄磁片中。已知的播放器包括讀取裝置，可讀取光學模型，以及回復裝置可回復中央標記的位元模型。播放器與資訊載體可形成一種系統來控制資訊重製。為此目的，播放器包括可獨立在中央標記上重製資訊的裝置。若資訊被拷貝在可寫入的資訊載體中，則此拷貝上的資訊不會被播放器所重製，因為在寫入程序中，只有光學模型會以預先定義的方法來寫入，而拷貝本身並不含任何中央標記。

(請先閱讀背面之注意事項再填寫本頁)

訂

## 五、發明說明(3)

本系統中所熟知的問題是，拷貝資訊之後無法有效控制重製資訊。若資訊包括該拷貝位元，則這類位元可以輕易地製造，例如在PC上或在小型電子電路上。含複製位元的資訊可以自由拷貝。若資訊以倒頻方式錄製時，則可利用中央標記位元模型在重製時解倒頻，資訊可以以其平板(解倒頻)的狀態來錄製，且完全不防拷貝。

本發明的目標在於提供一種系統，其中可控制拷貝，拷貝保護不會輕易地由位元複製而受到破壞。

為此目的，依本發明的系統，其特徵在於所拷貝的資訊具代表第二位元模型的水印，其中的第二位元模型與第一位元模型預定關連性，而播放器包括編碼器裝置，可在資訊中嵌入水印，以及可依第一與第二位元模型之間的關連性，產生第二位元模型的產生器裝置，該播放器包括可確認第一與第二位元模型之間的關連性的認證裝置。水印表示已錄製資訊的版權狀態。這麼作有一項好處，即為代表重製之後的資訊信號仍含有水印，而播放器可查覺到要錄製的提供的信號的版權狀態，但由水印代表的信號版權狀態則不能改變或在不擾信號的情形下複製。之前使用中央標記為解倒頻鍵或固定的密碼的技藝系統，無法讓"不法"的可錄製磁片具固定，錯誤的中央標記。例如，任何自倒頻錄製保護磁片中所讀取的資訊可以錄製在不法的拷貝中，在使用固定、錯誤鍵(重)倒頻之後。水印模型與中央標記位元模型之間的關連性需要中央標記與所錄製的資訊相串連才能達成。因此依照本發明的系統，不能用固定、

(請先閱讀背面之注意事項再填寫本頁)

訂

## 五、發明說明(4)

錯誤的中央標記來製造不法的拷貝。由於在第一(中央)位元模型與第二(水印)位元模型之間有預先定義的關連性，因此可實現堅強的拷貝保護，因為不法的拷貝必定含有與水印相關的特定中央標記，依預定的關連性，而因此可強迫不法集團獲取此關連性而加以更正。選擇合適的關連性可防止這類不法的拷貝。播放器水印的偵測很簡單，而自資訊載體讀取的資訊並不需要任何的加工程序，如解倒頻。水印位元標記的播放器認證可防止拷貝，且標記不容易被複製。另一項優點為播放器的認證功能進行緩慢，這是因為該預定關連性在啟動錄製資訊時的複製時，必須只能執行一次。

讀者應注意到，WO 97/13248-A1，在之前即已建檔，在本發明(PHN 15391，文件D2)之前日期發行之後，即說明影像信號的水印系統。可在磁片上錄製水印影像信號，該磁片包括一中央標記。然而，中央標記只表示中央類型，且與信號或水印無關。

本系統的較佳具體實施例的特徵在於，該關連性包括密碼圖解單向功能。單向功能可防止當所要的結果已知(如水印位元標記模式)，可以利用"向後"計算來發現源頭(如中央標記位元模型)。這樣作有其好處，不法集團被迫直接由原來媒介來獲取中央標記位元標記。他可能無法找到原來的媒介，或可能安裝播放器，使標記位元模型無法由外部取得。這樣會建立對試著製造中央標記"中文"拷貝不法集團的防護。

(請先閱讀背面之注意事項再填寫本頁)

訂

## 五、發明說明(5)

本發明的其他方面可參照以下所敘述的具體實施例與圖式以求更清楚的了解：

圖1說明條件性的重播規則，

圖2說明包括錄製器、中央標記、與播放器的錄製保護，

圖3說明單向功能，

圖4說明錄製器，與

圖5說明播放器。

我們提出儲存在儲存媒介，如DVD音效設備(數位影音光碟)的位元流或DSD-信號(直流數位)的拷貝控制方法。本方法有賴於水印方法，如由A.A.M. Bruekers等人所提出的方法之一，說明在相關文件表的文件D3中。最近，大家都了解到水印或嵌入式的信號可以用來作為拷貝保護方法，是防止盜錄的有效方法。水印或嵌入式的信號是一種可以在音頻內容之內埋藏資訊的方法。在本文中，我們使用由可靠團體所認可的產品專業文字，該類文字代表錄製工業與硬體製造商的焦點所在。本文亦標示出何種產品為消費性產品。消費性產品應遵循版權規則，接受執照合約或法律的約束。

對於拷貝保護需要全套的解決方案，水印並不限於數位格式，且可以嵌入類比信號並在類比信號中受到偵測。專家常建議使用分散頻譜科技來將水印嵌入音頻中。分散頻譜科技難題在於擷取或偵測此類資料需要實質的信號處理。雖然，這對專業設備使用在合法的案例以改進音頻材料上

(請先閱讀背面之注意事項再填寫本頁)

訂



## 五、發明說明(6)

並不成問題，但所需的電算能力卻不在消費性電氣產生可支援拷貝保護的範圍內。特定的問題在於，由音樂工業所設定的音頻品質要件需要大規模的分散增益，這樣同步與資料偵測才能增加其冗長的整合次數。在分散頻譜水印中所考慮的參數，預先假設並不能滿足目前的音頻品質要件，未來的標準鎖定在更加強音頻品質，並同時保護音樂IPR。我們均深深地相信，若要在不久的將來結合兩種滿意的方案來形成令人滿意的要件，且以合理的價格是不可能的。尤其是在所安裝的音頻設備缺乏保護裝置的情形下更會造成問題。要避免利用回到類比而進行信號拷貝更是不可能。更甚者，消費者所期待的是在家拷帶，如可在車內聆聽則有可能。因此，許多國家會在拷貝空白帶作為自己使用的情形課稅，某些限制類比拷貝的技術裝置是不合法的。因此需要設定新標準來儲存並代表數位音頻(如包括類比拷貝)，但可解決此項難題的科技不太可能馬上出現。因此可能會使用位元流解決方案，借由此項科技，可以有效保護新音頻儲存裝置並防止"中國人"(尤指中國大陸)盜拷新磁片，即使可能可以類比拷貝。為要拷貝，需要轉換至其他範疇(如，類比)而某些品質流失會出現。在此所提出的計畫是使用水印，不能解決現有的盜拷問題，而過分地在家拷帶亦會將音頻信號轉換為類比拷貝程序之一部分。若業者基於水印而採取拷貝保護裝置，則可預設為層化方法。最有力的水印應可忍受D/A與A/D的轉換，但卻必須花費較長的整合次數來偵測。這表示錄製或重播抑

(請先閱讀背面之注意事項再填寫本頁)

訂

## 五、發明說明(7)

制決策會受到遲滯。在位元流的水印可在毫秒之內被偵測出來，並立即觸動拷貝保護裝置。如此快速的偵測，若位元流信號在許多匯流排之間轉移(如P1394)，則會馬上出現。總而言之，在本文所描述的方法具以下特性：

- 有版權所有限制的位元流或DSD信號可以立即由家庭錄製中區別。

- 專業或消費性錄製器之可追蹤性。

- 可與其他方法並用以防止其他形式的拷貝(如類比)。尤其是，利用在此文所說明的方法以增加條件性的重放樂趣至條件性錄製方法，該方法可檢查分散頻譜水印。

在本發明中，我們主張保護高品質數位DSD位元流的直接保護拷貝，本方法不能技術地保護DSD轉換至PCM或類比的轉換。然而，在此提供了某些保護，若位元流/DSD信號被轉換回DSD，則DSD會被以消費性DSD編碼器的流水號被標以水印。本方法依靠水印方法，如由A.A.M. Bruekers等人所提出的計畫之一。本文的方法可與其他拷貝保護方法合併使用，包括序列拷貝管理位元與在分散頻譜水印中嵌入信號。消費性設備的額外硬體是非常小型的。使用在系統具體實施例的另一項工具為中央標記，如可辨認專業磁碟與可錄製磁碟的方法。此類工具的執行可為顫動鍵(如D1)，頻道密碼錯誤(如EFM)的調制或國際位元跳動調制與磁碟的接合區，或嵌入磁碟上的晶片，或寫入在引入區的資料無法由消費錄製者所存取。這兩種工具(水印與中央標記)可用來支援以下功能：

(請先閱讀背面之注意事項再填寫本頁)

訂

## 五、發明說明(8)

- 條件性的錄製是最常用來作為拷貝保護的方法，消費錄製者不能錄製內容，除非這類內容可以合法錄製。

- 條件性的重播，另一方面可接受某些人在盜版磁片上獲取可拷貝位元。

條件性的重播可確定這類盜版磁片不能在消費者播放器上重放，也就是說，盜拷者不能合法銷售這類磁片。在條件性的重播中，消費者DVD音頻播放器無法播放音頻磁片，若符合某一版權條件。播放器可確認音頻內容為消費者錄製或為專業發行音頻內容，利用檢查音頻流上的水印即可。在後者情形下(專業內容由版權所有保護)，播放器可檢查磁碟是否為原版並由專業人士錄製，而不是由消費錄製者或消費者磁碟媒體所拷貝。這樣需要內容的作標記方法(水印)與可標示實質儲存媒介的方法，該方法是只可以由專業錄製器或印刷機器才能製造的。

圖1說明嵌入在消費錄製器的條件性重播規則，該規則可應用在偵測到水印之後。當作為中央標記的第一標誌11出現時，通常為一實質標記，被讀取磁頭以不同於讀取錄製資訊的方法偵測到時，例如利用減調制該顫動。若中央標記出現了，則它會在第二標誌16中受到認證為有效的專業磁碟標記，若啟動播放17，若水印與中央標記依預定關連性而相連時。若中央標記不出現或表示消費錄製磁碟(以第三標誌12來表示)，則水印會在解碼器13受到解碼。水印可以表示自由拷貝(音頻)資訊，而後啟動磁碟的播放14。若水印表示防拷貝資訊，則播放動作會限於狀態

(請先閱讀背面之注意事項再填寫本頁)

訂

## 五、發明說明(9)

15。

在本系統的第一具體實施例中，專業製作的磁碟可以承載發行者特有的辨別器，該辨別器是不能拷貝的。辨別器因此可為一套的位元，寫入在錄製者無法存取的區域內，它可以是顫動鍵或在執行使用在DVD中的EFMplus頻道密碼的DC組件之特殊模型。DVD音頻播放器可檢查此一標記，若此標記無法得到，或若它包含家用磁碟錄製者所用的特殊水印，則它只會在找到特殊辨識DVD編碼器的水印時，才會重放DSD位元流。若找不到水印，或若專業發行的音頻流受到不法的拷貝至可錄製的磁碟上時，情形也是一樣。為要避免專業DSD品質的惡化，本方法並不需要專業發行的音頻標題標以水印，但此方法會需要將嵌入方法應用在消費者設備上。除了經常的重複拷貝控制位元之外，獨特的流水號碼亦由全部的DSD編碼器/錄製器在消費者市場中嵌入到音頻流中。嵌入此號碼的電路很簡單。消費者不將專業DSD音頻直接拷貝至DVD音頻磁碟中，正如它無法被播放一樣(因為沒有水印)。若他轉換信號為類比信號，PCM或其他種格式，則會重新創造DSD，可追蹤特定的DSD錄製者。更甚者，以此種裝置可定義較小的動態範圍。可更加強，若每台播放器不僅檢查水印是否出現在消費者磁片上，且檢查有效的流水號碼是否已嵌入。已知的密碼圖解方式可用來作為整合檢查，如連鎖數位簽名至流水號碼。這樣會避免盜拷者複製流水號碼。

第二具體實施例與第一具體實施例相似，但專業發行的

(請先閱讀背面之注意事項再填寫本頁)

訂

## 五、發明說明(10)

音頻位元流亦包括一水印。該水印是用來在密碼圖表方法中確認中央標記。中央標記與各標題不同，由水印所代表的位元模型與由中央標記所代表的位元模型之間的關連性並不容變更。較佳的密碼圖表關連性為，讓 $y=F(x)$ 與 $x=G(u)$ 為兩個密碼圖表單向功能，如它們的反函數為不可計算的，但必須與有限算術方法一併計算。本方法利用子晶 $u$ 來創造 $x$ 與 $y$ ，根據 $x=G(u)$ 與 $y=F(x)=F(G(u))$ 。在此概念中， $G$ 與 $F$ 可為同一種功能，但不一定為同一種功能。在專業錄製的磁片中，嵌入式的水印包括 $y$ 而中央標記則有 $x$ 。專業錄製器在寫入中央標記之前均會執行 $G$ 功能，也就是說，它們嵌入了中央標記 $x$ ，可由使用者輸入 $u$ 來內部產生。全部的(消費者)錄製器可執行 $F$ 以確認中央標記，若找到可表示內容是拷貝保護的水印。消費者錄製器假設無法寫入中央標記。利用本系統，版權所有的擁有者可以自行決定是否要釋放可允許複製的子晶 $u$ 。在專業的音樂發行中，必須建立音樂標題的磁帶標題。音頻以嵌入式的水印 $y$ 來預先編碼。在產生的程序中，專業錄製器(磁碟專業產生器機器)可直接接受具水印的DSD 30並在圖2的DSD編碼器/水印23之後插入。子晶 $u$  22亦在本程序中插入。若專業磁帶遭偷竊，則本方法亦可提供些許的保護，但 $u$ 則無法保證。較佳的情形是，錄製器檢查 $u$ 與 $x$ 上的水印(如圖4所示，為條件性錄製)。

圖2說明包括錄製器、資訊載體與播放器的拷貝保護系統。專業錄製器包括一音頻輸入端21可連至DSD編碼器

(請先閱讀背面之注意事項再填寫本頁)

訂

## 五、發明說明(11)

23中，該編碼器可將水印位元模型 $y$ 嵌入位元流30以在專業磁碟26上錄製。該水印位元模型 $y$ 可在產生器25的輸出端中取得，該產生器具位元模型 $x$ 由其輸入端的中央標記20來代表。中央標記20可在專業磁碟26中建立，較佳的情形是，位元模型 $x$ 由產生器24來產生，由在輸入端22的輸入子晶 $u$ 。專業磁碟26被一般的製造方法來加大，以拷貝受保護的資訊載體27，該資訊載體可在消費播放器28中播放出來。消費播放器28包括一確認器29，該確認器可比較受側的水印位元模型 $y$ 與計算數值 $y'$ ， $y'$ 是基於中央標記的偵測位元模型 $x$ 而算出來的。

在本方法中，拷盜者必須存取合法的專業錄製器，來在拷盜磁碟上建立中央標記。拷盜者可以拷貝音頻並回復 $y$ ，但他不能計算 $x$ 。本系統增加拷貝保護的安全性，尤其是在我們可以確定 $x$ 不能輕易地由磁碟上被讀取，例如在基本引擎上的第一片晶片(必須使用 $x$ 來確認水印 $y$ )。更甚者，即使拷盜者可以讀取 $x$ ，他必須找到 $u$ 以將它輸入至錄製器中，並讓 $x$ 當成中央標記以寫入。錄製器無法直接到 $x$ 並將其寫入到磁碟。以此方法，拷盜者必須修正他(合法登記的錄製)的錄製器(到旁通道G功能)以及其播放器(以選取 $x$ )。

在另一項具實施例中拷貝保護可以提供來給消費者錄製。可以看出若消費者要發行或小規模地散佈他們自己的音頻創造品。我們現在要描述消費錄製器如何能運用以上的裝置元件，這樣可讓消費者製造可以直接拷貝的磁片

(請先閱讀背面之注意事項再填寫本頁)

訂

## 五、發明說明(12)

(位元對位元)，若接收者亦知道子晶 $u$ 。部份的中央標記必須由接收者來錄製，可能的實施例可將 $x$ 分為兩個部份，為 $x=x_1||x_2$ ，如此一來 $y=F(x_1||x_2)$ 其中的 $x_1$ 為中央標記，相似以上所描述的方法，而 $x_2$ 可在磁片上以分開的檔案寫入。專業的錄製器可以寫入 $x_1$ 與 $x_2$ 。消費錄製器可以寫入 $x_2$ ，但在可錄製的磁片上， $x_1$ 具預設值 $x_1=x_c$ 可預先壓入在磁片中。消費錄製器可嵌入水印 $y=F(x_c||x_2)$ ，其中 $x_2$ 可由子晶 $u$ 產生，例如，利用採取 $G(u)$ 的位元部份。擁有者可以複製他自己的創造品，因為他知道 $u$ 。在播放器中， $x_1$ 與 $x_2$ 均不能離開基本的引擎，因此它可以為使用者而隱藏。

對於以上的具體實施例而言，水印模型與中央標記位元模型之間的關連性為單向功能。單向功能的實施可以為 $y=x^2$ 以共用模組來限制 $N$ 。在此的 $N$ 為兩個大保密素數( $N=pq$ )。事實上， $N$ 可以為部份的資料，該資料嵌入在水印中，例如，連鎖到 $y$ 。另一項可能性是，由Diffie與Hellman [1976](=文件D6)：所研究而成的不連續對數單向功能： $F(x)=\alpha^x$ 在 $GF(p)$ ，其中的 $\alpha$ 為 $GF(p)$ 之主要元素。其中的 $p$ 為主要元素，而 $p-1$ 具主要大的因子。以上兩種實施例均具理論上滿大的缺點，如需要保護的位元數。依較小位元而建立的實用系統可運用到合適的保密按鍵的模式中，如DES，其中的 $y=F(x)=x\otimes DES(x)$ ，此種情形說明在圖3的電路中。圖3說明單向功能產生器的實施，基於保密按鍵的模式。應用輸入端31中央標記位元模型 $x$ 並在加密器

(請先閱讀背面之注意事項再填寫本頁)

訂

## 五、發明說明(13)

32中處理，從按鍵33中使用按鍵。加密器32的輸出端為反位元方向EXOR'd到邏輯單位34的輸入端x，結果造成在輸出端35的位元模型y。在本電路中，該按鍵可以用公用方式來作成或包括在水印中，如連鎖至y中。

圖4說明消費者用的錄製器。錄製器具連接至DSD或PCM音頻編碼的編碼器42的類比音頻輸入端41，其中編碼器42可產生輸出位元流47以在可錄製磁碟48上錄製。位元模型y是由產生器43由位元模型x來產生，其中的x可由中央標記46來代表，並可能包括由預先壓縮的實質標記來擷取位元到可錄製的磁碟48上。錄製器具子晶輸入端45，該子晶u連接至產生器44以產生位元模型x。錄製器具第二輸入端40可讓數位音頻信號，連接至水印檢查器49。檢查器49可連接至產生器43以接收位元模型y並確認水印的出現。檢查器的基本的錄製控制功能可偵測到錄製，若偵測到專業的"非拷貝"水印。較好的情形是水印嵌入，當在數位輸入信號中並未偵測到水印。若出現水印，表示可以拷貝可拷貝的內容，若相對的子晶u應用至子晶輸入端45中。在不同的實施例中，消費錄製器只具有數位輸入端40與水印檢查器49，其中的類比輸入與水印編碼器並未出現。錄製器的另一項實施例與上述實施例相似，但不會以外部輸入端45來提供，但具內部u產生器，例如，隨機數字產生器。在此情形下，產生器44亦不會出現。

在單純的形式中，條件式的錄製裝置不會在重放時執行

(請先閱讀背面之注意事項再填錄本頁)

訂



## 五、發明說明(14)

檢查。在不同的實施例中，消費DSD錄製器接數類比信號，可能至某些類比拷貝資訊檢查。電路板上的DSD編碼器可以將水印嵌入至位元流中，水印包括二個部份：拷貝保護料以及序列辨識碼。消費DSD錄製器接收數位DSD位元流，只要它可以辨識有效拷貝控制資料。此拷貝控制資料應表示此資料可以合法地拷貝到磁片中。這類錄製器與圖4內的錄製器相仿，但不具有子晶輸入端45與產生器44。

消費DSD錄製器不接收包括拷貝控制標記的DSD位元流，該標記會阻止錄製。在較強的具體實施例中，拷貝控制資訊不出現會被認為是"不許拷貝"。在較弱的具體實施例中，沒有拷貝控制資訊的信號會被自動地重新選樣並加以水印。這樣會使拷貝保護減弱，且會降低品質。

在更進一步的實施例中更包括一拷貝功能，專業DSD位元流包括嵌入式的版權所有資料，該資料可允許一次的拷貝。可以利用更進一步的水印 $y_{co}$ (除了以上所描述的)。更甚者，專業磁碟上包括一特殊的許可標記 $x_{co}$ ，其中 $y_{co}=H(x_{co})$ ， $H()$ 為保密圖表單向功能。標記 $y_{co}$ 在重放時，仍保有音頻(可能已嵌入)，但它會由消費錄製器來移除。

圖5說明可自拷貝資訊載體51重製資訊的播放器52。播放器具讀取磁頭58與一般類型的讀取信號處理裝置，如光學磁頭，偵測器，頻道解碼器與CD或DVD光學磁片播放器的錯誤解碼器。播放器包括水印讀取裝置55，可偵測位元模型 $y$ 並由水印來代表，在資訊載體51中的已錄製的資

(請先閱讀背面之注意事項再填本頁)

訂

## 五、發明說明(15)

訊。位元模型y連接至邏輯單元54，該單元可運作來啟動切換器56。單元54的邏輯功能與條件性的重放規則已參照圖1而作過討論。播放器具裝置50可偵測中央標記並自水中擷取位元模型x，如利用如D1所說明的顫動模組。播放器更具認證裝置，可在位元模型x與位元模型y之間認證其預定的關連性。位元模型x連接至功能單元53以執行預定的功能F(x)，如單向功能。功能單元53的輸出端連接至邏輯單元54並與y比較。啟動切換器56通過已回復的音頻信號到輸出端57，若位元模型x與y的確說明該預定的關連性。

讀者應注意到利用條件性錄製的混合錄製可與條件性重放共同存在。本裝置的特殊方法是(除了在介紹文中所提及的技術性困難)，在類比範疇內的水印可以由錄製器來執行。若盜拷者試著要修正其錄製器以旁通此項條件式的錄製檢查，則可將專業DSD放在磁片上，此處所描述的拷貝保護即可防止錄製器上的內容流到市面上。

雖然本發明已說明利用DSD音頻來實施具體實施例，但仍可使用許多其他的音頻水印與或影像水印的實施例。亦可能在PCM音頻中使用水印。在LSB中的隱藏資料中，可能包括效果的光譜形狀。這類嵌入式裝置的執行可參照Oomen等人在1994年所發表的文件(D4)。此種嵌入式裝置的應用方式，我們最好能在有限的預選樣本中嵌入資料，以一位元對一選定樣本。這類嵌入式方法可以在相同的裝置中執行，而將專業(24位元)音頻轉換為低解析度(如16

(請先閱讀背面之注意事項再填寫本頁)

訂

## 五、發明說明(16)

位元)。之前所提及的DSD水印方法(D3)可以用來將資料嵌入至PCM中。另一項選擇是使用較少流失的嵌入式信號。較少流失的編碼方法是由Bruekers等人提出(描述在D5中)。另一種嵌入資料的方法是，依水印規則來選擇預定濾波器的屬性與參數(圖10，D5的152項)。例如，數位水印"1"可以為代表，利用擇濾波器分接頭的單數號，而"0"則作為分接頭的偶數號碼。在另一項實施例中，依相仿規則濾波器係數受到數量化。更進一步，平均信息量編碼器可以利用轉換其參數來嵌入資料，這類嵌入至PCM信號的信號可用來建構基於之前概念的拷貝保護方法。盜拷者不再能拷貝壓縮的PCM位元對位元到磁片上並將之在市場上銷售。他必須經過解壓縮與壓縮的程序，雖然這不會造成品質損害(因為編碼為較少流失)，它仍可造成不同的數位信號，最後的檔案將包括更多的位元，若消費錄製器可以較不具效率的方法來壓縮，而結果的檔案會包括有關錄製器的流水號碼的資訊。

在本實施例中，已說明磁片與資訊載體，但其他的載體亦可使用在此發明中，如卡帶或廣播，只要供應中央標記的方法不會輕易地被盜拷。其他的發明可有新式的功能與多種功能的結合。

(請先閱讀背面之注意事項再填寫本頁)

訂

## 五、發明說明 (17)

## 相關文件表

- (D1) EP-0545472 (PHN 13922)  
具實質拷貝保護的密閉式資訊系統
- (D2) WO 97/13248-A1 (PHN 15391)  
水印編碼信號
- (D3) EP-A 97200197.8建檔日期27.01.97 (PHN 16209)  
位元流-或DSD-信號的水印製作(A.A.M. Bruekers等人)
- (D4) 美國專利5,649,054 (PHN 14700)  
隱藏式資料頻道
- (D5) WO IB97/01156 (PHN 16452)  
DVD音頻的較少流失編碼(A.A.M. Bruekers等人)
- (D6) 密碼圖表的新方向(Dieffie與Hellman)，資訊理論的  
IEEE交換期刊，Vol IT-22，No. 6，1976年11月，  
p.644-654

(請先閱讀背面之注意事項再填寫本頁)

訂

## 六、申請專利範圍

1. 一種已錄製資訊之拷貝保護的系統，包括一含中央標記的資訊載體，該中央標記代表第一位元模型(x)，一錄製器可在資訊載體上錄製資訊，而播放器可重製資訊載體上的已錄製的資訊，其特徵在於已錄製的資訊包括代表第二位元模型(y)的一水印，該第二位元模型與第一位元模型相關，該第二位元模型包括一編碼器裝置(23)，可將水印嵌入資訊中，及一產生器裝置(25)，可依第一與第二位元模型的關連性產生第二位元模型，該播放器包括一確認裝置(29)，可確認第二位元模型與第一位元模型之間的關連性。
2. 如申請專利範圍第1項的系統，其特徵在於其關連性包括一密碼單向功能。
3. 如申請專利範圍第2項的系統，其特徵在於利用提供單向功能至第一位元模型(x)而產生第二位元模型(y)。
4. 如申請專利範圍第1，2，或3項的系統，其特徵在於第二位元模型確認編碼器裝置。
5. 一種使用在申請專利範圍第1，2或3項系統中的錄製器，可在資訊載體上錄製資訊，該資訊載體包括一中央標記，代表第一位元模型(x)，其特徵在於錄製器包括編碼器裝置(42)，可將水印嵌入資訊中，該水印代表第二位元模型(y)，而產生器裝置(43)可依第一與第二位元模型之間的關連性而產生第二位元模型。
6. 如申請專利範圍第5項的錄製器，其特徵在於包括一標記裝置(46)，可在資訊載體上建立中央標記，而產生器

(請先閱讀背面之注意事項再填寫本頁)

訂

線

專利申請案  
修正本  
有變更  
內容者  
是否准予修正  
89年9月18日所製

經濟部中央標準局員工消費合作社印製

六、申請專利範圍

1. 一種已錄製資訊之拷貝保護的系統，包括一含中央標記的資訊載體，該中央標記代表第一位元模型(x)，一錄製器可在資訊載體上錄製資訊，而播放器可重製資訊載體上的已錄製的資訊，其特徵在於已錄製的資訊包括代表第二位元模型(y)的一水印，該第二位元模型與第一位元模型相關，該第二位元模型包括一編碼器裝置(23)，可將水印嵌入資訊中，及一產生器裝置(25)，可依第一與第二位元模型的關連性產生第二位元模型，該播放器包括一確認裝置(29)，可確認第二位元模型與第一位元模型之間的關連性。
2. 如申請專利範圍第1項的系統，其特徵在於其關連性包括一密碼單向功能。
3. 如申請專利範圍第2項的系統，其特徵在於利用提供單向功能至第一位元模型(x)而產生第二位元模型(y)。
4. 如申請專利範圍第1，2，或3項的系統，其特徵在於第二位元模型確認編碼器裝置。
5. 一種使用在申請專利範圍第1，2或3項系統中的錄製器，可在資訊載體上錄製資訊，該資訊載體包括一中央標記，代表第一位元模型(x)，其特徵在於錄製器包括編碼器裝置(42)，可將水印嵌入資訊中，該水印代表第二位元模型(y)，而產生器裝置(43)可依第一與第二位元模型之間的關連性而產生第二位元模型。
6. 如申請專利範圍第5項的錄製器，其特徵在於包括一標記裝置(46)，可在資訊載體上建立中央標記，而產生器

(請先閱讀背面之注意事項再填寫本頁)

訂

線

專利申請案  
本有無變更實質內容是否准予修正。  
89年9月18日所製之

經濟部中央標準局員工消費合作社印製

## 六、申請專利範圍

包括可依預定的關連性來產生子晶(u)的第一位元模型的裝置(44)。

7. 如申請專利範圍第6項的錄製器，其特徵在於產生器(43)利用結合，由在可錄製的資訊載體的預壓縮的標記表示之第一部份( $x_c$ )與由子晶(u)所產生的第二部份( $x_2$ )來產生第一位元模型(x)。
8. 如申請專利範圍第7項的錄製器，其特徵在於預定關連性包括一密碼單向功能。
9. 一種用於申請專利範圍第1，2或3項系統的資訊載體，該資訊載體(51)包括一已錄製的資訊與一代表第一位元模型(x)的中央標記(50)，其特徵在於已錄製的資訊包括一代表第二位元模型(y)的水印，該水印對第一位元具預先定義的關連性。
10. 如申請專利範圍第9項的資訊載體，其特徵在於第一位元模型包括可確定資訊載體的來源的第一部份( $x_c$ )，與可確認( $x_t$ )的第二部份。
11. 一種用於申請專利範圍第1，2或3項系統的播放器，可重製資訊載體(51)的資訊，並包括可偵測出中央標記的裝置(50)，該中央標記代表第一位元模型(x)，其特徵在於該播放器包括一水印讀取裝置(55)，可偵測由在錄製資訊中的水印所代表的第二位元模型(y)，而在此情形下，該播放器包括確認裝置(53，54)可確認第二位元模型與第一位元模型之間的預定關係。
12. 如申請專利範圍第11項的播放器，其特徵在於認證裝置

(請先閱讀背面之注意事項再填寫本頁)

訂

線

## 六、申請專利範圍

包括一密碼圖表單向功能(53)。

13. 如申請專利範圍第12項的播放器，其特徵在於編程認證裝置，來產生確認模型( $y'$ )，只要利用將單向功能運用至第一位元模型( $x$ )，並包括可比較確認模型( $y'$ )與第二位元模型( $y$ )的裝置(54)。

(請先閱讀背面之注意事項再填寫本頁)

訂

線



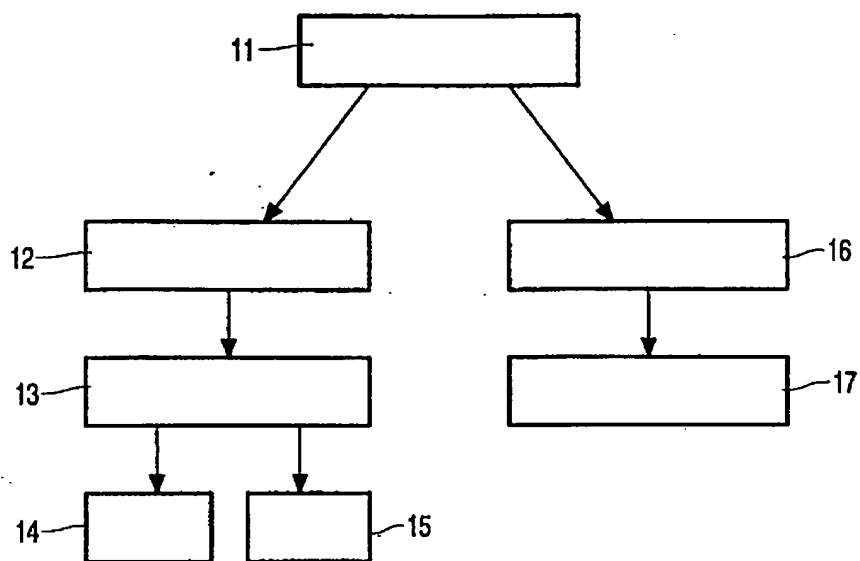


圖 1

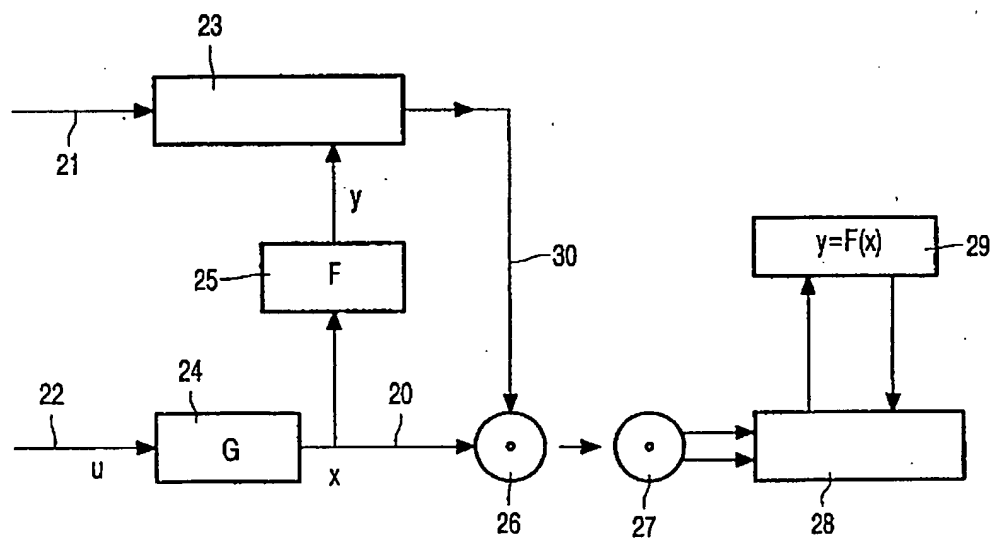


圖 2

428163

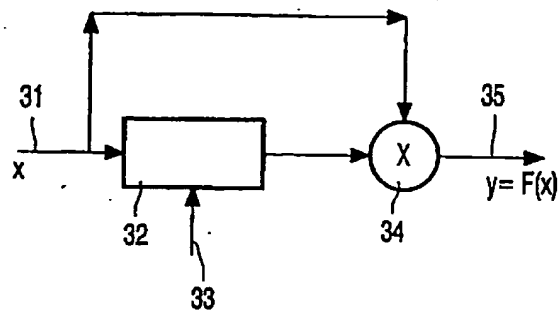


圖 3

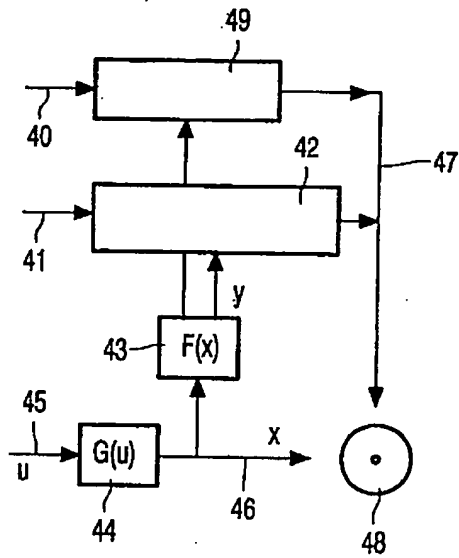


圖 4

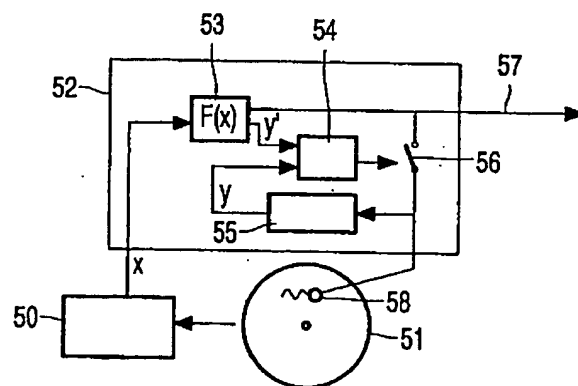


圖 5

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☒ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**